AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions and listings of claims in the application.

1. (Presently Amended) A method for preventing unauthorized distribution of a software application program comprising a plurality of files downloaded from a server platform to a client platform, the client platform comprising a plurality of hardware components, over a distributed network, comprising:

installing a client software program on the client platform, the client software program performing a first sequence comprising:

establishing a communications channel between the client platform and the server platform;

retrieving a plurality of identifying indicia associated with the client platform;

formatting the identifying indicia to create a unique user identifier associated with the client platform; and

transmitting the unique user identifier to the server platform on the communications channel;

~~encrypting the software application program using the unique user identifier~~ embedding at the server platform the unique user identifier into the software application program;

transmitting the software application program from the server platform to the client platform; and

installing the software application program on the client platform.

2. (Original) The method of claim 1, wherein the step of installing the client program comprises downloading the client program from the server platform over a first communications channel.

3. (Original) The method of claim 1, wherein the second communications channel is an encrypted communications channel.

4. (Original) The method of claim 1, wherein the identifying indicia comprises at least one identification number, which is associated with at least one hardware component of the client platform.

5. (Original) The method of claim 1, wherein each identifying indicia is associated with at least one hardware component.

6. (Original) The method of claim 5, wherein the step of formatting the identifying indicia into a unique user identifier, comprises:

    concatenating the identifying indicia; and

    formatting the concatenated identifying indicia as a hexadecimal string.

7. (Presently Amended) The method of claim 1, ~~wherein~~ further comprising ~~the step of encrypting the unique user identifier into the software application program, comprises~~:

    parsing the unique user identifier into a plurality of segments;

    embedding each segment into a separate file associated with the software application program;

    encrypting each separate file; and

    generating an encryption key.

8. (Original) The method of claim 7, wherein the step of parsing the unique user identifier in to a plurality of segments comprises MD5 hashing the unique user identifier into 16-bit words.

9. (Presently Amended) The method of claim [1] 7, wherein the step of transmitting the software application program to the client platform comprises:

    transmitting each encrypted file associated with the software application program to the client platform; and

transmitting the encryption key to the client platform.

10. (Original) The method of claim 9 further comprising downloading the encrypted files and encryption key over the encrypted communications channel.

11. (Presently Amended) The method of claim [1] 10, wherein the step of installing the software application program on the client platform comprises:

determining a number of separate locations on a media storage device equal to the number of encrypted files downloaded; and

writing each encrypted file in a predetermined order to the separate locations of a media storage device associated with the client platform to insure that the software application programs runs correctly.

12. (Presently Amended) The method of claim [1] 7, further comprising:

performing a first sequence each time the software application program is run on a client platform, comprising;

retrieving each segment of the parsed unique user identifier from each file associated with the software application program;

recombining the retrieved segments to create the unique user identifier;

retrieving the identifying indicia associated with the client platform;

generating a unique user identifier for the client platform;

comparing the recombined unique user identifier with the unique user identifier generated from the client platform;

running the software application program if the recombined unique user identifier matches the unique user identifier generate from the client platform; and

terminating the software application program is if the recombined unique user identifier does not match the unique user identifier generate from the client platform.

13. (Original) The method of claim 1, further comprising:
determining whether the client application program has been previously executed;

if the determination is made that the client applications program has previously been executed, terminating the client application program and the software application program; and

if the determination is made that the client application program has not been previously executed, performing the first sequence.

14. (Original) The method of claim 13, wherein the step of determining whether the client application program has been previously executed, comprises:

establishing an encrypted communications link with the platform server after the client application program has been executed;

passing the unique user identifier to the server;

comparing the unique user identifier with the each unique user identifier stored in the memory storage device associated with platform server;

if the determination is made that the unique user identifier matches at least one unique user identifier previously stored in the memory storage device, terminating the client application program; and

if the determination is made that the unique user identifier does not match at least one unique user identifier store in the memory storage device, performing the first sequence.

15. (Presently Amended) A method for preventing the unauthorized distribution of software applications programs, comprising:

installing a first control program on an authorized computer, the first control program operable for performing a first sequence in response to the control program being executed, the first sequence comprising;

generating a unique user identifier in response to the plurality of hardware devices associated with the authorized computer; and

transmitting the unique user identifier to a remote computer, wherein the remote computer contains a second control program operable to determine whether the first control program has previously been executed;

in response to determining that the first control program has not been previously executed, the second control program performing a second sequence, subsequent to the first sequence, comprising;

embedding at the remote computer the unique user identifier into the software application program; and

transmitting the software application program to the authorized machine[;] .

16. (Presently Amended) A system for preventing unauthorized distribution of a software application program, comprising:

a distributed network;

a client platform connected the distributed network, the client platform operable for executing a client program, which is operable for generating a unique user identifier (UUI) associated with the client platform; and

an application server platform connected to the distributed network, the application server platform operable for;

receiving the UUI from the client platform at the application server platform and embedding the UUI into a plurality of files associated with the software application program; and downloading the plurality of files from the application server platform to the client platform.